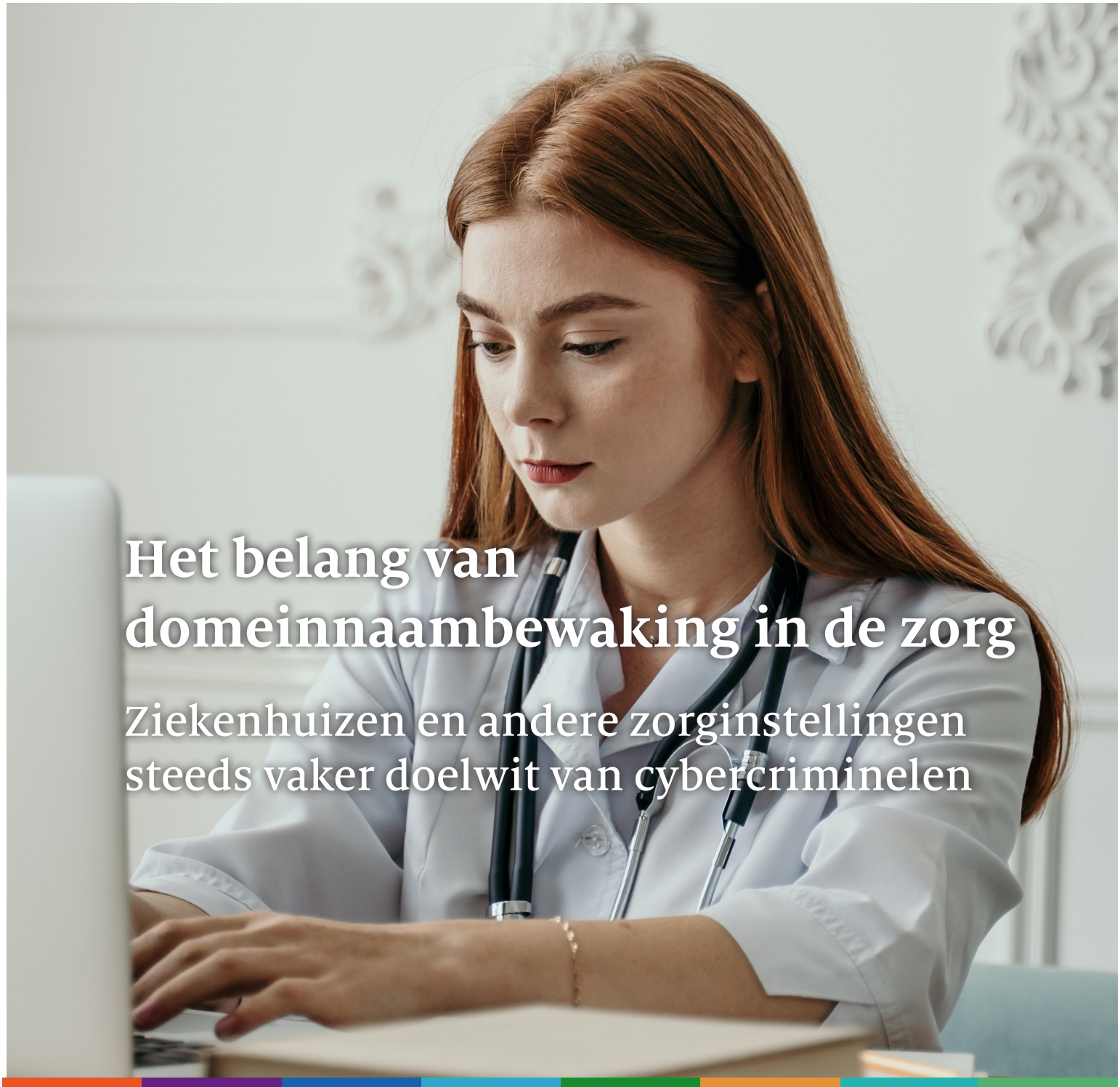


Het belang van domeinnaambewaking in de zorg

Ziekenhuizen en andere zorginstellingen steeds vaker doelwit van cybercriminelen

Zorginstellingen zijn zich steeds meer bewust van online dreigingen. Niet alleen van cybercriminelen die via phishing proberen patiëntgegevens te bemachtigen, maar ook van derden die de reputatie van de instelling schade willen berokkenen. Begin dit jaar sloegen experts al alarm over het **toenemende aantal incidenten** in de zorg. Daarbij speelden malafide domeinnamen een grote rol. Een goed domeinnamenbeleid en actieve monitoring van nieuwe domeinnaamregistraties zijn daarom ook in de zorg belangrijk. Maar hoe omvangrijk is het probleem nu echt? Wij doorzochten hiervoor alle 6,2 miljoen .nl-domeinnamen op overeenkomsten met de namen van 10 grote ziekenhuizen. Een 'smoking gun' vonden we gelukkig niet, maar genoeg aandachtspunten.

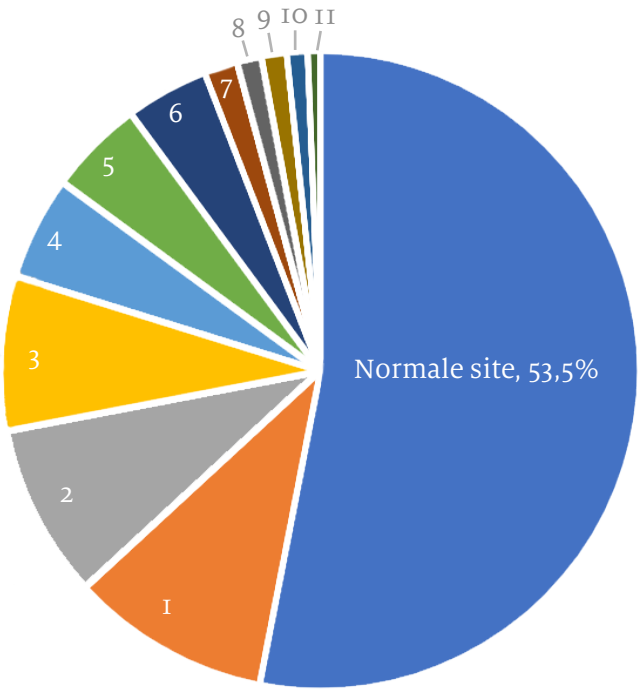
23 verdachte domeinnamen, geen smoking gun

Het percentage phishingsites is in .nl en Nederland al jaren stabiel tussen de 2 en 4% van alle domeinnamen, maar wel met een kanttekening: phishingwebsites worden steeds sneller offline gehaald. De kans dat je op een specifiek moment een actieve phishingwebsite vindt is dus niet groot. Vaak zie je een ongebruikte domeinnaam die lijkt op de naam van een zorginstelling, maar niet door die instelling geregistreerd wordt.

Een voorbeeld uit ons onderzoek is de domeinnaam **jeroenbosziekenhuis.nl.** Een domein dat niet gebruikt wordt of op naam staat van het Jeroen Bosch Ziekenhuis in 's-Hertogenbosch, maar waarvan de overeenkomsten met de échte naam en domeinnaam (jeroenboschziekenhuis.nl) van het ziekenhuis wel heel sterk zijn. Ook de domeinnaam i**kaziaziekenhuis.nl** is opvallend, omdat deze wel heel duidelijk naar een bestaand ziekenhuis verwijst, maar niet op naam van dat ziekenhuis staat. Genoemd ziekenhuis gebruikt ikazia.nl.

Tip!

Voor sommige vormen van fraude wordt de malafide domeinnaam vaak doorgelinkt naar de site van de organisatie waarvan de identiteit misbruikt wordt. Cybercriminelen doen dit, omdat slachtoffers de domeinnaam ter controle intypen, op een legitieme site komen en denken dat de ontvangen phishingmail bonafide is. Ontdek je een domeinnaam die een typo op je merknaam is en opeens verkeer naar je website begint te verwijzen? Dan is het raadzaam deze nader te onderzoeken.



Tabel 1: Domeinnamen die sterk lijken op namen van 10 grote Nederlandse ziekenhuizen (Bron: SIDN, november 2021)

1. Reageert niet - 10,1%
2. Ongebruikt - 8,8%
3. Geparkeerde site - 7,8%
4. 'Te koop' site -5,3%
5. Phising site - 4,8%
6. Redirect naar originele domeinnaam - 4,2%
7. Adult - 1,7%
8. Alleen e-mail - 1,3%
9. Verwijderd - 1,3%
10. Reclamenetwerk -1,1%
11. Niet van toepassing - 0,6%

Het grijze gebied: reputatieschade

Zeker bij zorginstellingen speelt het belang van een goede reputatie. Bij ons onderzoek troffen wij veel domeinnamen aan met twijfelachtige intenties. Bijvoorbeeld: **‘<naamziekenhuis>-doofpot.nl’.** Ook het te koop aanbieden van domeinnamen met de merknaam erin is, hoewel niet illegaal, mogelijk wel in strijd met het intellectueel eigendomsrecht. Zo stond de domeinnaam **zuiderland.nl** ten tijde van ons onderzoek te koop.

Zeker bij zorginstellingen speelt het belang van een goede reputatie.

Ongewenst ‘bonafide gebruik’

Veel zorginstellingen zijn voortgekomen uit fusies en overnames. Hierdoor zijn domeinnamen in het verleden vaak op veel verschillende plaatsen geregistreerd, waardoor overzicht ontbreekt. Ook registreren maatschappen vaak hun eigen domeinnamen binnen een instelling. Dit kan tot misverstanden en problemen leiden.

Een voorbeeld is onderstaande lijst van domeinnamen behorend bij een van de onderzochte ziekenhuizen:

<naamziekenhuis>.nl	<afdeling ICT>
<naamziekenhuis>apotheek.nl	<afdeling ICT>
<naamziekenhuis>expo.nl	<Ziekenhuis>
<naamziekenhuis>expo.nl	<Ziekenhuis>
<naamziekenhuis>jaarverslag.nl	<extern bureau>
<naamziekenhuis>routewijzer.nl	<extern bureau>
<naamziekenhuis>ziekenhuis.nl	<Provider>
<naamziekenhuismet typefout>.nl	<particulier>
<naam>-ikazia.nl	<maatschap (?)>

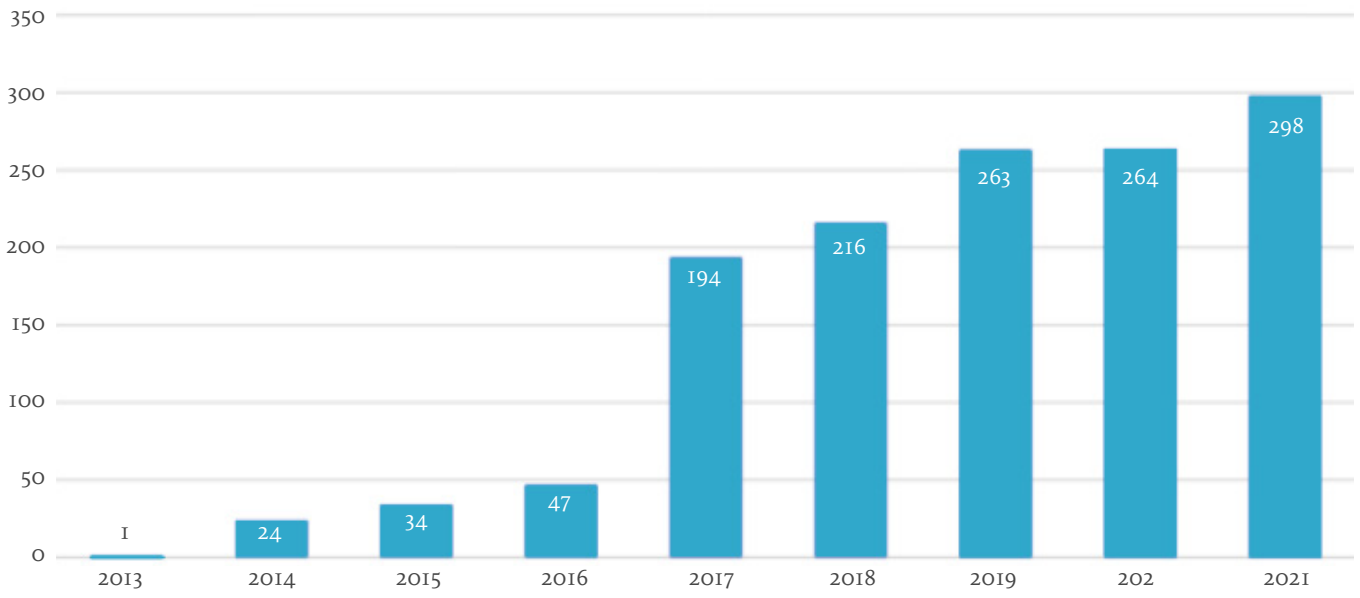
Een dergelijke diversiteit in tenaamstelling van de gebruikte domeinnamen kan tot misverstanden leiden bij gebruikers en maakt centraal beheer, bijvoorbeeld door een SOC, lastig. Dit kan bijvoorbeeld tot problemen leiden bij het verlengen van certificaten of het implementeren van veilige mailstandaarden.

Verlopen domeinnamen

Veel domeinnamen belanden in verkeerde handen door misverstanden bij de zorginstelling zelf. Meest voorkomend is het geval waarin de instelling van naam wijzigt, maar de oude domeinnaam verbonden blijft met online toegankelijke applicaties. Een voorbeeld is de pijnlijke case van **Bureau Jeugdzorg Utrecht** dat van naam veranderde en waar journalisten mailadressen aanmaakten met behulp van een oude domeinnaam. Met die mailadressen (vb. <naammedewerker>@bureaujeugdzorg.nl) gingen ze naar een online applicatie en vroegen een herstel van hun wachtwoord aan. Dat herstel slaagde, waarna ze toegang kregen tot een groot aantal cliëntendossiers. Om herhaling te voorkomen bracht brancheorganisatie Z-CERT dit jaar een zeer bruikbare **handreiking verlopen domeinnamen** voor zorginstellingen uit.

Tools ontwikkelen mee

De handreiking van Z-CERT betreft het beheer van eigen domeinnamen. Maar wat doe je tegen van buitenaf geregistreerde malafide domeinnamen? Of eigen domeinnamen waar men het bestaan niet van weet. Steeds meer organisaties in de publieke sector gebruiken daar domeinnaambewakingstools voor. Zo wordt SIDN Merkbewaking in Nederland al gebruikt om 300 grote merken te bewaken. En de technologie die we gebruiken om cybercriminelen op te sporen wordt steeds beter. Zo kunnen wij vanaf 2022 ook logo's op mogelijk malafide websites detecteren en komt er een nieuwe crawler, waarmee zoekresultaten nauwkeuriger geclassificeerd worden. Dit verkleint de kans dat een phishingwebsite door de mazen van het net glipt.



Tabel 2: Aantal grote Nederlandse merknamen dat gebruik maakt van SIDN Merkbewaking (Bron: SIDN)

Wat te doen als je merkmisbruik spot?

Veel organisaties zijn zich er onvoldoende van bewust dat ze ook zonder tussenkomst van de rechter tegen online merkmisbruik kunnen optreden. Voor .nl is die geschillenregeling te vinden op **sidn.nl**. Dat is meestal goedkoper, makkelijker en sneller dan naar de rechter. De registry's voor .com en andere niet-landgebonden extensies vind je op de website van de verantwoordelijke registry of op **ICANN.org**.

Bewaak je merk online!

Aandacht voor online gebruik van de eigen merk- of handelsnaam blijft dus belangrijk. Het voeren van een actief domeinnamenbeleid en regelmatig domeinnaamregistraties monitoren die lijken op de naam van je bedrijf horen daarbij. Ook het beveiligen van mail met veilige internetstandaarden zoals DMARC moet prioriteit krijgen. Zorginstellingen moeten zich realiseren dat elk bedrijf, ook de kleinere, een interessant doelwit kan zijn voor cybercriminelen en zich hierop voorbereiden.

	.nl	.com (en andere niet-landgebonden extensies)
Inbreuk op intellectueel eigendomsrecht	• Geschillenregeling voor .nl-domeinnamen • Rechter	Uniform Domain Name Dispute Resolution Policy (ICANN.org)
Onrechtmatige content	• Notice-and-Take-Down-procedure (EU)	Notice-and-Take-Down-procedure (US)
Klacht over registrar	• Geschillencommissie	Uniform Domain Name Dispute Resolution Policy (ICANN.org)

Tabel 3: De opties voor een geschil rond domeinnamen

Wat is SIDN Merkbewaking?

Met SIDN Merkbewaking waarschuwen wij je vooraf over de registratie van een domeinnaam die lijkt op jouw merk. Dan kun je in actie komen voordat een aanval op je merk start of voordat je merk last krijgt van look-a-likes of identiteitsfraude. Ook hou je controle over interne registraties en registraties van businesspartners. Zo voorkom je reputatieschade en hoge kosten.

SIDN Merkbewaking meldt jou de .nl-domeinnamen voordat deze beschikbaar zijn op het internet. Domeinnamen van andere toplevels zoals .com en .org ontvang je binnen 24 uur. Met SIDN Merkbewaking handel je eenvoudig de resultaten af via jouw persoonlijke dashboard. De workflow en een automatische indeling per categorie ondersteunen je hierbij. Je kunt met de tool ook juridische expertise inschakelen en de opvolging van zaken eenvoudig vastleggen. Er is ook een eenvoudige feed, die je per mail op de hoogte houdt.

Als gebruiker van SIDN Merkbewaking kun je met een additionele module direct juridische actie ondernemen op verdachte domeinnamen die door SIDN Merkbewaking gedetecteerd zijn. Deze module geeft je toegang tot de diensten van ICTRecht: gespecialiseerde juristen op het gebied van online misbruik en merkinbreuk. Op de juridische opvolging zijn de algemene voorwaarden van ICTRecht van toepassing. Bekijk de actuele versie van de voorwaarden van ICTRecht.

Meer informatie

Wil je meer weten over dit onderzoek of over SIDN Merkbewaking? Neem dan contact op met Peter Rotgans, specialist domeinnaammonitoring, via peter.rotgans@sidn.nl of kijk op **www.sidn.nl/sidn-merkbewaking.**

Neem contact op met:

Peter Rotgans
peter.rotgans@sidn.nl
+31 26 352 55 55

Met SIDN Merkbewaking waarschuwen wij je vooraf over de registratie van een domeinnaam die lijkt op jouw merk.